IN THE ABSTRACT

Methods and systems to provide support for single stepping a virtual machine in a virtual machine environment are disclosed. ~~In one embodiment, a~~ An exemplary method may includes receiving a request to transition control to a virtual machine (VM) from a virtual machine monitor (VMM), determining that a single-stepping indicator is set to a single stepping value, and transitioning control to the VM. Further, if an execution of a first instruction in the VM completes successfully, control is transitioned to the VMM following the successful completion of the execution of the first instruction.

IN THE CLAIMS

1. (Currently Amended) A method comprising:

receiving a request to transition control to a virtual machine (VM) from a virtual machine monitor (VMM);

determining that a single-stepping indicator is set to a single stepping value;

transitioning control to the VM; and

if an execution of a first instruction in the VM completes successfully, transitioning control to the VMM following the successful completion of the execution of the first instruction, without requiring any user interaction between receiving the request to transition control to the VM and transitioning control back to the VMM.

2. (Original) The method of claim 1 wherein transitioning control to the VMM comprises informing the VMM that control is transitioned to the VMM due to a current value of the single-stepping indicator.

3. (Original) The method of claim 1 further comprising:

if the execution of the first instruction in the VM does not complete successfully due to a current fault, determining whether the current fault caused by the execution of the first instruction is associated with a transition of control to the VMM.

4. (Original) The method of claim 3 further comprising:

if the current fault is associated with the transition of control to the VMM, transitioning control to the VMM, and informing the VMM that control is transitioned to the VMM due to the current fault.

5. (Original) The method of claim 3 further comprising:

if the current fault is not associated with the transition of control to the VMM, delivering the current fault to the VM; and

if the delivery of the current fault completes successfully, transitioning control to the VMM prior to executing any instructions of a corresponding fault handler, and informing the VMM that control is transitioned to the VMM due to a current value of the single-stepping indicator.

6. (Original) The method of claim 5 further comprising:

determining that the delivery of the current fault was unsuccessful;

determining whether a new fault is associated with a transition of control to the VMM; and

if the new fault is associated with the transition of control to the VMM, transitioning control to the VMM, and informing the VMM that control is transitioned to the VMM due to the new fault.

7. (Original) The method of claim 6 further comprising:

determining that the new fault is not associated with the transition of control to the VMM;

delivering the new fault to the VM; and

if the delivery of the new fault completes successfully, transitioning control to the VMM prior to executing any instructions of a corresponding fault handler, and informing the VMM that control is transitioned to the VMM due to a current value of the single-stepping indicator.

8. (Original) The method of claim 1 further comprising:

prior to transitioning control to the VM, determining that the request to transition control to the VM is associated with a vectored fault to be delivered to the VM;

delivering the vectored fault to the VM when transitioning control to the VM; and

if the delivery of the vectored fault completes successfully, transitioning control to the VMM vectored to executing any instructions of a corresponding fault handler, and informing the VMM that control is transitioned to the VMM due to a current value of the single-stepping indicator.

9. (Original) The method of claim 8 further comprising:

determining that the delivery of the vectored fault was unsuccessful;

determining whether a new fault is associated with a transition of control to the VMM;

if the new fault is associated with the transition of control to the VMM, transitioning control to the VMM, and informing the VMM that control is transitioned to the VMM due to the new fault; and

if the new fault is not associated with the transition to the VMM, delivering the new fault to the VM, transitioning control to the VMM prior to executing any instructions of a corresponding fault handler, and informing the VMM that control is transitioned to the VMM due to a current value of the single-stepping indicator.

10. (Original) The method of claim 1 further comprising:

prior to transitioning control to the VM, determining that the request to transition control to the VM is associated with a non-active activity state of a processor;

transitioning control to the VM; and

refraining from transitioning control to the VMM until after an occurrence of a break event.

11. (Original) The method of claim 10 further comprising:

if the break event is associated with a transition of control to the VMM, transitioning control to the VMM, and informing the VMM that control is transitioned to the VMM due to the break event.

12. (Original) The method of claim 10 further comprising:

determining that the break event is not associated with a transition of control to the VMM;

delivering the break event to the VM;

if the delivery of the break event completes successfully, transitioning control to the VMM prior to executing any instructions of a corresponding handler, and informing the VMM that control is transitioned to the VMM due to a current value of the single-stepping indicator; if the delivery of the break event was unsuccessful,

determining whether a new fault is associated with a transition of control to the VMM;

if the new fault is associated with the transition of control to the VMM, transitioning control to the VMM, and informing the VMM that control is transitioned to the VMM due to the new fault; and

if the new fault is not associated with the transition of control to the VMM, transitioning control to the VMM prior to executing any instructions of a corresponding fault handler, and informing the VMM that control is transitioned to the VMM due to a current value of the single-stepping indicator.

13. (Original) The method of claim 1 wherein the single stepping indicator is included in a virtual machine control structure (VMCS).

14. (Original) The method of claim 1 further comprising:

prior to transitioning control to the VMM, accessing a save activity state indicator, and saving a specifier of an activity state of the VM if the save activity state indicator is set to a save value.

15. (Original) The method of claim 1 further comprising:

detecting, following the execution of first instruction, an event having a higher priority than single stepping;

determining whether the higher priority event is to be handled by the VMM;

if the higher priority event is to be handled by the VMM, transitioning control to the VMM, and informing the VMM that control is transitioned to the VMM due to the higher priority event; and

if the higher priority event is not to be handled by the VMM, setting a pending VM exit indicator to a single stepping value, and transitioning control to software designated to handle higher priority events.

16. (Original) The method of claim 15 wherein the designated software delivers a pending VM exit due to a current value of the single stepping indicator to the VMM.

17. (Original) The method of claim 15 wherein the designated software requests the processor to deliver a pending VM exit due to a current value of the pending VM exit indicator to the VMM.

18. (Original) The method of claim 15 further comprising:

detecting, after the designated software completes operation, that a VM exit due to a current value of the single-stepping indicator is pending;

transitioning control to the VMM; and

informing the VMM that control is transitioned to the VMM due to the current value of the single-stepping indicator

19. (Currently Amended) An apparatus comprising:

a virtual machine monitor (VMM);

a data structure controlled by the VMM, the data structure storing a single stepping indicator; and

single stepping logic to receive a request to transition control to a virtual machine (VM) from the VMM, to determine that the single-stepping indicator is set to a single stepping value, and, if an execution of a first instruction in the VM completes successfully, to transition control to the VMM following the successful execution of the first instruction, without requiring any user interaction between receiving the request to transition control to the VM and transitioning control back to the VMM.

20. (Original) The apparatus of claim 19 wherein the single stepping logic is to inform the VMM that control is transitioned to the VMM due to a current value of the single-stepping indicator.

21. (Original) The apparatus of claim 19 wherein the single stepping logic is further to determine whether a current fault caused by the execution of the first instruction is associated with a transition of control to the VMM, and, if the current fault is associated with the transition of control to the VMM, to transition control to the VMM and to inform the VMM that control is transitioned to the VMM due to the current fault.

22. (Original) The apparatus of claim 21 wherein the single stepping logic is further to deliver the current fault to the VM if the current fault is not associated with the transition of control to the VMM, and, if the delivery of the current fault completes successfully, to transition control to the VMM prior to executing any instructions of a corresponding fault handler and to

inform the VMM that control is transitioned to the VMM due to a current value of the single-stepping indicator.

23. (Currently Amended) A system comprising:

a memory to store one or more indicators; and

a processor, coupled to the memory, to use the one or more indicators to determine that single stepping of a virtual machine (VM) is indicated, to execute a first instruction in the VM, and, if the execution of the first instruction completes successfully, to transition control to a virtual machine monitor (VMM) following the successful completion of the execution of the first instruction, without requiring any user interaction between receiving the request to transition control to the VM and transitioning control back to the VMM.

24. (Original) The system of claim 23 wherein the processor is to inform the VMM that control is transitioned to the VMM due to a current value of the single-stepping indicator.

25. (Original) The system of claim 23 wherein the processor is further to determine whether a current fault caused by the execution of the first instruction is associated with a transition of control to the VMM, and, if the current fault is associated with the transition of control to the VMM, to transition control to the VMM and to inform the VMM that control is transitioned to the VMM due to the current fault.

26. (Original) The system of claim 25 wherein the processor is further to deliver the current fault to the VM if the current fault is not associated with the transition of control to the VMM, and, if the delivery of the current fault completes successfully, to transition control to the VMM

prior to executing any instructions of a corresponding fault handler and to inform the VMM that control is transitioned to the VMM due to a current value of the single-stepping indicator.

27. (Currently Amended) An article of manufacture comprising a machine-readable storage medium containing instructions which, when executed by a processing system, cause the processing system to perform a method, the method comprising:

receiving a request to transition control to a virtual machine (VM) from a virtual machine monitor (VMM);

determining that a single-stepping indicator is set to a single stepping value;

transitioning control to the VM; and

if an execution of a first instruction in the VM completes successfully, transitioning control to the VMM following the successful completion of the execution of the first instruction, without requiring any user interaction between receiving the request to transition control to the VM and transitioning control back to the VMM.

28. (Original) The machine-readable medium of claim 27 wherein transitioning control to the VMM comprises informing the VMM that control is transitioned to the VMM due to a current value of the single-stepping indicator.

29. (Original) The machine-readable medium of claim 27 wherein the method further comprises:

if the execution of the first instruction in the VM does not complete successfully due to a current fault, determining whether the current fault caused by the execution of the first instruction is associated with a transition of control to the VMM.

30. (Original) The machine-readable medium of claim 29 wherein the method further comprises:

if the current fault is associated with the transition of control to the VMM, transitioning control to the VMM, and informing the VMM that control is transitioned to the VMM due to the current fault.